

Joshua Adam Schulte, *pro se*

May 2, 2022

BY HAND

Judge Jesse M. Furman
United States District Judge
Southern District of New York
40 Foley Square
New York, New York 10007

RE: *United States v. Joshua Adam Schulte, S3 17 Cr. 548 (JMF)*

Dear Judge Furman:

I respectfully submit this letter in reply to the government's response dated April 29, 2022, Dkt. 791, regarding the mirror images.

I. Dr. Bellovin's affidavits are accurate

The government first claims that Dr. Bellovin's February 22, 2020 affidavit "inaccurately claimed that the Government had not made certain data available." Got. Letter at 2. The government never corrected the forensic case file—to this date it still displays files modified by the government's review on November 6, 2018; the other forensic artifacts in that case file are tainted and unreliable. However, the government did provide some of the original, unmodified files and selected unallocated space as a separate production outside the forensic case.

Regardless, the purpose of this paragraph was to highlight the fact that overall data integrity cannot be assured without access to the mirror images. See Bellovin Aff. ¶ 32 ("While the government now asserts it has corrected this issue, the underlying question of the integrity of the mirror images remains; without the mirror images, the defense cannot confirm whether the government followed proper forensic protocols or otherwise tainted and destroyed relevant data.").

Next, the government claims that Dr. Bellovin's statement regarding the private key is false. See Bellovin Aff. ¶ 36 ("At trial, Mr. Leedom testified about Mr. Schulte's encrypted private SSH key. But Mr. Leedom did not verify that Mr. Schulte's private key corresponded to the public key file, and I was not able to do it myself because I lacked access to machine-readable and processable copies of the files purported to be Mr. Schulte's private and public

United States v. Schulte, S3 17 Cr. 548 (JMF); May 2, 2022 letter from pro se defendant

SSH keys.”). Mr. Leedom did not actually perform the fingerprint to the jury, but simply testified that he did. Dr. Bellovin cannot confirm this testimony because he is unable to reproduce Mr. Leedom’s test as he has no digital copies of the keys. This is the primary point of contention—Dr. Bellovin has essentially been reduced to an observer who cannot rely upon his own expertise and experience to do anything; instead, he must simply take Mr. Leedom and Mr. Berger’s analysis, tests, and conclusions all at face value.

The government then claims that Dr. Bellovin’s statement about Mr. Berger’s timing analysis is inaccurate. See Bellovin Aff. ¶ 17 (“One of the major analyses performed by Mr. Berger that I could not reproduce without access to the stash and confluence backups stored on the FS01 Server was his ‘timing analysis’ (Tr. 1351-52). Mr. Berger relied upon all backups to note each day particular files were modified, and which of these versions were ultimately released by WikiLeaks. However, because of the way Stash works, that test is insufficient. With a version control system, it is possible to extract files as they existed at any time in the past to compare different versions of the Stash backups to the leaked Stash files. Furthermore, under certain circumstances, changes that appear to have been made on a given date might actually have been made considerably earlier.”). Mr. Berger stated in his affidavit that he “reconstituted the Stash database from the most recent available backup file” Berger Aff. ¶ 7. This is the same thing as “rely[ing] upon all backups.” Due to version control, the most recent backup contains the data from all previous backups. Dr. Bellovin was simply explaining Git and Stash in such a way that a non-technical person could understand it; Mr. Berger had access to all the data contained in all the backups to conduct his timing analysis. Whether the government provides this (which it has yet to do) by physically producing all the backups or simply providing the most recent, the result would be the same.

Finally, the government claims that “[o]ther aspects of the Dr. Bellovin Affidavit, if not entirely incorrect, are at least misleading.” They then only provide one example: Dr. Bellovin’s assertion that “I was given just several hours at a CIA facility to examine a redacted version of a few backup files.” Bellovin Aff. ¶ 16. While the government claims this is misleading, it then confirms Dr. Bellovin’s assertion by admitting to redactions. The government claims the only redactions it made were to usernames of CIA employees, but of course there is no possible way

United States v. Schulte, S3 17 Cr. 548 (JMF); May 2, 2022 letter from pro se defendant

for Dr. Bellovin to confirm how many redactions or what redactions the government made. The only fact that Dr. Bellovin knows for certain is that he did not receive a “mirror image” of the backup, but was provided a modified, redacted form of the data.

Contrary to Mr. Berger’s assertions that Dr. Bellovin does “not appear to have [expertise] in digital forensics,” Dr. Bellovin is a professor of computer science at Columbia University, who has not only been involved in both civil and criminal cases as a forensic expert, but has published extensively about forensics. Dr. Bellovin’s credentials are far superior to either Mr. Berger or Mr. Leedom, who does not even have a Master’s degree. Dr. Bellovin is considered a god among computer engineers such as myself; Dr. Bellovin worked at Bell Labs and AT&T Labs during the advent of the modern information age, is a Cybersecurity Hall of Famer, and was awarded the Usenix Lifetime Achievement Award for creating Usenet. There are few alive today with credentials equal to Dr. Bellovin.

II. The Defendant has shown that the government must either produce the mirror images of its case-in-chief or should otherwise be precluded from relying upon any testimony about those mirror images at trial

The government once again falsely claims that it has “already produced to the defendant and his expert the March 3, 2016 backups that the [g]overnment alleges were stolen and transmitted to WikiLeaks, first on December 10, 2018, and again on the standalone computer made available to Dr. Bellovin in November 2019.” Govt. Letter at 4. The government, however, never produced any Stash backups on December 10, 2018, and only provided a Confluence backup *with literally all the CIA materials redacted*. See Bellovin Decl. ¶ 7 (“...Instead, I received select files from the three servers (including from virtual machines hosted on the ESXi server) and redacted copies of the March 3, 2016 and March 4, 2016 Confluence backup files.”); see also Bellovin Decl. ¶ 15 (“The government provided the defense redacted Confluence backups from March 3, 2016 and March 4, 2016. The government removed all CIA content from these backups, so the defense was unable to perform any analyses or tests.”); see also Bellovin Decl. ¶ 33 (“The government claims that it provided the Confluence databases to the defense. But those databases appear to have been heavily redacted, with all content files either missing or deleted, including those allegedly released by

United States v. Schulte, S3 17 Cr. 548 (JMF); May 2, 2022 letter from pro se defendant

WikiLeaks.”). While the government asserts that it also provided the April 25, 2016 Confluence Backup, this backup also contains no files and is completely worthless. The government never provided the Stash backup, and essentially never provided the Confluence backup since all relevant CIA files were removed.

The government claims it provided less redacted versions of the Stash and Confluence backups to Dr. Bellovin through the CIA, but of course that is insufficient. As an initial matter, there is absolutely no precedent or case the government cites to assert this is a lawful discovery production. Fed. R. Crim. P. 16 does not contain a provision allowing the government to produce discovery in a restricted environment outside the jurisdiction of not only the district court but the presiding court of appeals. This is absolutely absurd. Furthermore, I have stated on the record that I have both a right and desire to review the backups the government alleges I stole. I have a Constitutional right for the government to provide me the very materials it alleges I stole—both the Fifth Amendment right to due process and the Sixth Amendment right to put forth a complete defense compel disclosure.

Mr. Berger’s testimony that a “competent expert” could review the standalone computer at the CIA obviously does not apply to the “forensic case” materials provided to me in the SCIF. It’s also not possible to conduct queries of the SQL database, because the manner in which the backups were produced at the SCIF. The forensic evidence provided in the SCIF is provided as a “forensic case” as defined by Dr. Bellovin’s affidavit: “Forensic Image or Forensic Case: A forensic image is standard forensic software, such as the AccessData Forensic Toolkit used by the government. A forensic image extracts and indexes files from a mirror image or from ‘free space’ on the disk.” Bellovin Decl. ¶ 6.b. Since these are not “mirror images” the defense cannot freely access the materials to perform basic analyses such as SQL queries.

To the degree the government now agrees it will provide an unredacted copy of the April 25, 2016 Confluence backup, so long as it is provided in the SCIF as a complete forensic copy, and not on the restricted “forensic case” server, it is certainly a step in the right direction. However, the government has not provided the Stash backup. The charges related to stash are the more serious, yet they produced the Confluence backup but not the Stash backup.

United States v. Schulte, S3 17 Cr. 548 (JMF); May 2, 2022 letter from pro se defendant

The government spends the majority of its letter discussing the Stash and Confluence backups, but otherwise fails to discuss the three servers it alleges to be at the heart of its case-in-chief: My CIA Workstation, the ESXi Server, and the FS01 Server.

III. The government is incorrect to equate forensic examinations to “searches of the government’s files” and provides no relevant case precedent

The government continues to equate a forensic examination to a “search of the government’s files.” However, this is not the relevant inquiry as there is very little case precedent of digital forensics and forensic examinations. See Omnibus Reply at 9-10:

The primary point of contention is the fact that digital forensics is a science that depends upon interpretation by experts. Lawyers, the Court, and the jury cannot competently and independently review computer forensics as if it were a simple stack of papers to read; experts are required to conduct forensic examinations, interpret and analyze the data, and form *testable* expert opinions based upon the complete forensic record. Accordingly, the government’s repeated assertions equating the forensic crime scene to mere “government records,” Opp. at 38, and reliance on cases from the 1980s involving hardcopy documents is inapposite and irrelevant. Moreover, the government itself argued the critical importance of obtaining the *complete* forensic image of digital devices for experts to conduct *full forensic examinations*—which this circuit acknowledged. See *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016). Indeed, forensic images of the *alleged crime scene* are not mere “government records” any more than DNA, hair samples, or clothing fibers found at the scene of the crime. Could the government argue the DNA discovered at a murder scene are “government records” that the defense cannot access or review? Could the government claim its own experts can review the DNA, and testify at trial that the DNA belongs to the defendant while simultaneously refusing to allow defense experts equal access to analyze the DNA and present its own conclusions? Thus why is it acceptable to do so for digital forensics?

Digital forensics is more closely related to forensic science. It is well-established that experts are necessary to conduct independent analysis on fingernail scrapings, blood, fingerprints, DNA, and other biological materials. No court has ever held that the defense must accept whatever findings and conclusions made by government experts. Instead, the defense is allowed to hire its own experts with “equal access” to materials tested by the government.

Moreover, the government does not cite a single case, in any district court, where the government asserted a defendant was not entitled to a “mirror image” of the alleged crime scene. Be it child pornography, Computer Fraud and Abuse, or any other computer-related

United States v. Schulte, S3 17 Cr. 548 (JMF); May 2, 2022 letter from *pro se* defendant

crime; in every single case the government has always produced a “mirror image” and turned them over in discovery. In no other case in the history of the United States has the government every indicted an individual for computer fraud and other computer crimes, provided its own experts access to the digital forensic crime scene, but refused equal access to the defense. See also Bellovin Decl. ¶ 10 (“Compared to the data made available to its own expert, the production to the defense is minuscule and far from complete. In no other case has my review been so limited in scope.”); ¶ 39 (“In all my experience, including civil litigation and a criminal prosecution in which I worked with the FBI, they always provided me with a mirror image copy of the suspect’s disks.”). The government’s own forensic experts agreed that this is “an atypical forensic review process.” Leedom Decl. ¶ 5; see also Leedom Decl. ¶ 6 (“... it is true that the most complete mirror image is typically the starting point for digital forensic analysis.”); Leedom Decl. ¶ 12 (“It is also true that as part of my role in reviewing the evidence collected in this case, I had access to additional information.”).

Thus, the same case precedent set forth in forensic sciences is relevant to digital forensics here. Indeed, Dr. Bellovin notes “that forensic examiners are not infallible. The only way I can test if the government made a mistake in their analysis, missed critical data, or otherwise misinterpreted data is through equal access to the mirror images and adversarial testing.” Bellovin Decl. ¶ 39. See also Omnibus Reply at 10:

The most important and distinguishing characteristic of both forensic science and digital forensics is that the prosecutors cannot determine whether *Brady* material exists—instead, they rely upon the analysis of their forensic experts—analysis that could be wrong, biased, or intentionally fabricated. Indeed, independent analysis is as necessary for digital forensics as it is for other forensic sciences or any field of expertise. “More and more, forensic evidence plays a decisive role in criminal trials today. But it is hardly ‘immune from the risk of manipulation.’” *Stuart v. Alabama*, 139 S. Ct. 36 (2018) (quoting *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 318 (2009)). “A forensic analyst ‘may feel pressure—or have an incentive—to alter the evidence in a manner favorable to the prosecution.’” *Ibid.* “Even the most well-meaning analyst may lack essential training, contaminate a sample, or err during the testing process.” See *ibid*; see also *Bullcoming v. New Mexico*, 564 U.S. 647, 654 n.1 (2011) (documenting laboratory problems). “To guard against such mischief and mistake and the risk of false convictions they invite, our criminal justice system depends on **adversarial testing and cross-examination.**” (emphasis added). *Ibid.* Accordingly, Mr. Schulte is entitled to adversarial testing and independent analysis—he need not put his faith entirely into the hands of government

United States v. Schulte, S3 17 Cr. 548 (JMF); May 2, 2022 letter from *pro se* defendant

experts, who are clearly not incentivized to “find” holes in their theories, evidence outside their bias, or exculpatory evidence helpful to Mr. Schulte. Only by subjecting the government’s case-in-chief to adversarial testing can Mr. Schulte receive a fair trial and justice be done.

Thus the government’s expert’s affidavits are largely unhelpful as they are self-serving declarations of what they *believed* to be relevant, and altogether different from what they considered relevant to their own review. See, e.g. Leedom Decl. ¶ 5 (“I am certain that the materials that have been provided to the defense are sufficient for a competent digital forensic expert to review and examine the facts to which I testified, and to verify or dispute the conclusions that I drew from those facts, to which I also testified at the trial in this matter in 2020.”); ¶ 6 (“Although the forensic artifacts pertaining to the daily backup files were relevant to my analysis, the overwhelming majority of other files on the NetApp were not relevant.”). Mr. Leedom also explains that “the vast majority of my conclusions and testimony in this case was not based on ‘tests’ I ran. On the contrary, and particularly with regard to the defendant’s activities on DEVLAN... My testimony... was based on my training and experience.” Leedom Decl. ¶ 7. But of course, Mr. Leedom was the one who searched and identified the files in unallocated space, picked out the log files he deemed were relevant, and otherwise had free reign to determine what he thought would be helpful to the government. Dr. Bellovin was not allowed to conduct his own examination, based upon his own training and experience.

The only relevant precedent regarding “equal access” is also in Mr. Schulte’s favor. The Supreme Court noted in *Wardius v. Oregon*, 412 U.S. 470 (1973), that “[a]lthough the Due Process Clause has little to say regarding the amount of discovery which the parties must be afforded, ...it does speak to the *balance of forces* between the accused and his accuser.” (emphasis added). Accordingly, “*Wardius* holds that rules about pretrial discovery in criminal prosecutions must apply to prosecutors as well as to defendants. **Access provided to private experts retained by the prosecution must be provided to private experts retained by the defense.**” *United States v. Shrake*, 515 F.3d 743 (7th Cir. 2008) (emphasis added).

Ultimately, the bottom line is Mr. Schulte is severely prejudiced without “equal access” to the same materials the government experts reviewed. Simply put, if the data requires an expert to make sense of it, then the government must provide it to the defense to conduct its

United States v. Schulte, S3 17 Cr. 548 (JMF); May 2, 2022 letter from *pro se* defendant

own tests. See Bellovin Decl. ¶ 38 (“The mirror images of the Schulte Workstation, ESXi Server, and FS01 Server are also critical to reconstruct the timeline of events. Mr. Leedom testified extensively to the timeline of events that he discovered upon analysis of the servers and Mr. Schulte’s Workstation. I was unable to reproduce the same results nor did I have an opportunity to conduct my own forensic examination and reconstruct my own timeline. An independent forensic examination could prove a different version of events altogether. Mr. Schulte’s alleged actions of utilizing his workstation to access the ESXi server, then the Confluence Virtual Machine, and ultimately steal backups from the FS01 server cannot be truly tested without equal access to these systems.”).

If the Court does not order either preclusion or discovery of the “mirror images,” then Mr. Schulte’s expert can only testify that he did not receive “equal access” to the “mirror images,” and therefore was unable to conduct the same tests as the government, cannot refute or confirm the government’s expert’s testimony, and cannot present his own conclusions. In effect, the Court essentially denies Mr. Schulte an expert at all. “[A] criminal trial is fundamentally unfair if the State proceeds against an indigent defendant without making certain that he has access to the raw materials integral to the building of an effective defense.” *Ake v. Oklahoma*, 470 U.S. 68, 77 (1985). Accordingly, the Court should order the government to produce the complete “mirror images” of the Schulte Workstation, ESXi Server, FS01 Server. Alternatively, the Court should preclude the government from introducing any evidence or testimony derived from these servers or any other electronics that it did not provide equal access to the defense.

Respectfully submitted,

Joshua Adam Schulte

A handwritten signature in black ink, appearing to read "Joshua Adam Schulte". The signature is fluid and cursive, with a large, stylized 'J' at the beginning.